

CM-Points on Straight Lines

Bill Allombert, Yuri Bilu, Amalia Pizarro-Madariaga

October 31, 2014

Abstract

We prove that, with “obvious” exceptions, a CM-point $(j(\tau_1), j(\tau_2))$ cannot belong to a straight line in \mathbb{C}^2 defined over \mathbb{Q} . This generalizes a result of Kühne, who proved this for the line $x_1 + x_2 = 1$.

Contents

1	Introduction	1
2	Imaginary Quadratic Orders	3
3	Ring Class Fields and Complex Multiplication	4
4	Comparing two CM-fields	7
5	Proof of Theorem 1.2	10

1 Introduction

In this article τ with or without indices denotes a quadratic¹ complex number with $\text{Im}\tau > 0$ and j denotes the j -invariant.

In 1998 André [1] proved that a non-special irreducible plane curve in \mathbb{C}^2 may have only finitely many CM-points. Here a *plane curve* is a curve defined by an irreducible polynomial equation $F(x_1, x_2) = 0$, where F is a polynomial with complex coefficients. A *CM-point* in \mathbb{C}^2 is a point of the form $(j(\tau_1), j(\tau_2))$ with quadratic τ_1, τ_2 . *Special curves* are the curves of the following types:

- “vertical lines” $x_1 = j(\tau_1)$;
- “horizontal lines” $x_2 = j(\tau_2)$;
- *modular curves* $Y_0(N)$, realized as the plane curves $\Phi_N(x_1, x_2) = 0$, where Φ_N is the modular polynomial of level N .

Clearly, each special curve contains infinitely many CM-points, and André proved that special curves are characterized by this property.

André’s result was the first non-trivial contribution to the celebrated André-Oort conjecture on the special subvarieties of Shimura varieties; see [12] and the references therein.

Independently of André the same result was also obtained by Edixhoven [8], but Edixhoven had to assume the Generalized Riemann Hypothesis for certain L -series to be true.

Further proof followed; we mention specially the remarkable argument of Pila [11]. It is based on an idea of Pila and Zannier [13] and readily extends to higher dimensions [12].

The arguments mentioned above were non-effective, because they used the Siegel-Brauer lower bound for the class number. Breuer [5] gave an effective proof, but it depended on GRH.

Recently Kühne [9, 10] and, independently, Bilu, Masser, and Zannier [4] found unconditional effective proofs of André’s theorem. Besides giving general results, both articles [10] and [4] treat also some particular curves, showing they have no CM-points at all. For instance, Kühne [10, Theorem 5] proves the following.

¹“Quadratic” here and below mean “of degree 2 over \mathbb{Q} ”.

Theorem 1.1 *The straight line $x_1 + x_2 = 1$ has no CM-points.*

(The same result was also independently obtained in an earlier version of [4], but did not appear in the final version.)

A similar result for the curve $x_1x_2 = 1$ was obtained in [4].

One can ask about CM-points on general straight lines defined over \mathbb{Q} ; that is, defined by an equation

$$A_1x_1 + A_2x_2 + B = 0, \quad (1)$$

where $A_1, A_2, B \in \mathbb{Q}$. One has to exclude from consideration the *special straight lines*: $x_1 = j(\tau_1)$, $x_2 = j(\tau_2)$ and $x_1 = x_2$, the latter being nothing else than the modular curve $Y_0(1)$ (the modular polynomial Φ_1 is $x_1 - x_2$). According to the theorem of André, these are the only straight lines containing infinitely many CM-points.

In the present paper we obtain a rather vast generalization of Theorem 1.1.

Theorem 1.2 *Let $(j(\tau_1), j(\tau_2))$ be a CM-point belonging to a non-special straight line defined over \mathbb{Q} . Then we have one of the following options. Either*

$$j(\tau_1), j(\tau_2) \in \mathbb{Q}, \quad (2)$$

or

$$j(\tau_1) \neq j(\tau_2), \quad \mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2)), \quad [\mathbb{Q}(j(\tau_1)) : \mathbb{Q}] = [\mathbb{Q}(j(\tau_2)) : \mathbb{Q}] = 2. \quad (3)$$

Remark 1.3 1. Recall that $[\mathbb{Q}(j(\tau)) : \mathbb{Q}] = h(\mathcal{O}_\tau)$, the class number of the “complex multiplication order” $\mathcal{O}_\tau = \text{End}\langle \tau, 1 \rangle$, where $\langle \tau, 1 \rangle$ is the lattice generated by τ and 1. All orders of class number 1 and 2 are well-known, which means that points satisfying (2) or (3) can be easily listed. In fact, there are 169 CM-points satisfying (2) and, up to \mathbb{Q} -conjugacy, 217 CM-points satisfying (3); see Remark 5.3 for the details.

2. Our result is best possible because any point satisfying (2) or (3) does belong to a non-special straight line defined over \mathbb{Q} .
3. Kühne remarks on page 5 of his article [10] that his Theorem 4 allows one, in principle, to list all possible CM-points belonging to non-special straight lines over \mathbb{Q} , but the implied calculation does not seem to be feasible.
4. Bajolet [2] produced a software package for finding all CM-points on a given straight line. He illustrated its efficiency by proving that no straight line (1) with non-zero $A_1, A_2, B \in \mathbb{Z}$ satisfying $|A_1|, |A_2|, |B| \leq 10$ passes through a CM-point. This work is now formally obsolete because of our Theorem 1.2, but a similar method can be used in more general situations, where our theorem no longer applies.
5. CM-points (x_1, x_2) satisfying $x_1x_2 \in \mathbb{Q}^\times$ are completely classified in [3]; this generalizes the above-mentioned result from [4] about the curve $x_1x_2 = 1$.

In Sections 2 and 3 we recall basic facts about imaginary quadratic orders, class groups, ring class fields and complex multiplications.

In Section 4 we investigate the field equality $\mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2))$. In particular, in Corollary 4.2 we determine all cases of such equality when $\mathbb{Q}(\tau_1) \neq \mathbb{Q}(\tau_2)$. This might be of independent interest.

After all these preparations, we prove Theorem 1.2 in Section 5.

Acknowledgments. We thank Lars Kühne whose marvelous article [10] was our principal source of inspiration. We also thank Karim Belabas, Henri Cohen, Andreas Enge and Jürg Kramer for useful conversations, and the referee for the encouraging report and many helpful comments.

Yuri Bilu was supported by the *Agence National de la Recherche* project “Hamot” (ANR 2010 BLAN-0115-01). Amalia Pizarro-Madariaga was supported by the ALGANT scholarship program.

Our calculations were performed using the PARI/GP package [17].

2 Imaginary Quadratic Orders

In this section we recall basic facts about imaginary quadratic fields and their orders, and recall a famous result of Weinberger about class groups annihilated by 2.

2.1 Class Groups

Let K be an imaginary quadratic field and \mathcal{O} an order in K of discriminant $\Delta = Df^2$, where D is the discriminant of the field K (often called the *fundamental discriminant*) and f is the conductor of \mathcal{O} , defined from $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$. We denote by $\text{Cl}(\mathcal{O})$ the class group of \mathcal{O} (the group of invertible fractional ideals modulo the invertible principal fractional ideals). As usual, we set $h(\mathcal{O}) = |\text{Cl}(\mathcal{O})|$. Since \mathcal{O} is uniquely determined by its discriminant Δ , we may also write $\text{Cl}(\Delta)$, $h(\Delta)$ etc. In particular, $\text{Cl}(D) = \text{Cl}(\mathcal{O}_K)$ is the class group of the field K , and $h(D)$ is the class number of K .

There is a canonical exact sequence

$$1 \rightarrow \text{Cl}_0(\Delta) \rightarrow \text{Cl}(\Delta) \rightarrow \text{Cl}(D) \rightarrow 1, \quad (4)$$

where the kernel $\text{Cl}_0(\Delta)$ will be described below. This implies, in particular, that $h(D) \mid h(\Delta)$.

The structure of the group $\text{Cl}_0(\Delta)$ is described, for instance, in [7], Section 7.D and Exercise 7.30. We briefly reproduce this description here. We will assume, with a slight abuse of notation, that $\mathbb{Z}/f\mathbb{Z}$ is a subring of $\mathcal{O}_K/f\mathcal{O}_K$. Then have another canonical exact sequence

$$1 \rightarrow (\mathbb{Z}/f\mathbb{Z})^\times (\mathcal{O}_K^\times)_f \hookrightarrow (\mathcal{O}_K/f\mathcal{O}_K)^\times \rightarrow \text{Cl}_0(\Delta) \rightarrow 1, \quad (5)$$

where $(\mathcal{O}_K^\times)_f$ is the image of the multiplicative group \mathcal{O}_K^\times in $(\mathcal{O}_K/f\mathcal{O}_K)$.

The group $(\mathbb{Z}/f\mathbb{Z})^\times (\mathcal{O}_K^\times)_f$ is “not much bigger” than $(\mathbb{Z}/f\mathbb{Z})^\times$. Precisely,

$$[(\mathbb{Z}/f\mathbb{Z})^\times (\mathcal{O}_K^\times)_f : (\mathbb{Z}/f\mathbb{Z})^\times] = [\mathcal{O}_K^\times : \mathcal{O}^\times] = \begin{cases} 2 & \text{if } D = -4, f > 1, \\ 3 & \text{if } D = -3, f > 1, \\ 1 & \text{otherwise.} \end{cases}$$

An easy consequence is the following formula for $h(\Delta)$:

$$h(\Delta) = \frac{fh(D)}{[\mathcal{O}_K^\times : \mathcal{O}^\times]} \prod_{p \mid f} \left(1 - \left(\frac{D}{p}\right) p^{-1}\right), \quad (6)$$

where (D/\cdot) is the Kronecker symbol.

2.2 Orders with Class Groups Annihilated by 2

In this subsection we recall the famous result of Weinberger about imaginary quadratic orders whose class group is annihilated by 2. For a multiplicatively written abelian group G we denote by G^2 its subgroup of squares: $G^2 = \{g^2 : g \in G\}$.

The group $\text{Cl}(\Delta)/\text{Cl}(\Delta)^2$ is usually called the *genus group* of Δ . It is known to be isomorphic to $(\mathbb{Z}/2\mathbb{Z})^\mu$, where $\mu = \mu(\Delta) \in \{\omega(\Delta) - 1, \omega(\Delta)\}$ and $\omega(\cdot)$ denote the number of distinct prime divisors. We may also remark that $\mu(\Delta) = \omega(\Delta) - 1$ when $\Delta = D$ (and $f = 1$).

Already Euler studied discriminants Δ with the property

$$|\text{Cl}(\Delta)^2| = 1, \quad (7)$$

or, equivalently, $\text{Cl}(\Delta) \cong (\mathbb{Z}/2\mathbb{Z})^\mu$. (Of course, he used a different terminology.) Chowla proved that the set of such Δ is finite. Using a deep result of Tatzawa [14] about Siegel’s zero, Weinberger [16] improved on this, by showing that *field discriminants* D with this property are bounded explicitly with at most one exception.

Table 2.1: Known Δ with $|\text{Cl}(\Delta)^2| = 1$

$h(\Delta) = 1$	$-3, -3 \cdot 2^2, -3 \cdot 3^2, -4, -4 \cdot 2^2, -7, -7 \cdot 2^2, -8, -11, -19, -43, -67, -163$
$h(\Delta) = 2$	$-3 \cdot 4^2, -3 \cdot 5^2, -3 \cdot 7^2, -4 \cdot 3^2, -4 \cdot 4^2, -4 \cdot 5^2, -7 \cdot 4^2, -8 \cdot 2^2, -8 \cdot 3^2, -11 \cdot 3^2,$ $-15, -15 \cdot 2^2, -20, -24, -35, -40, -51, -52, -88, -91, -115, -123, -148,$ $-187, -232, -235, -267, -403, -427$
$h(\Delta) \geq 4$	$-3 \cdot 8^2, -7 \cdot 8^2, -8 \cdot 6^2, -15 \cdot 4^2, -15 \cdot 8^2, -20 \cdot 3^2, -24 \cdot 2^2, -35 \cdot 3^2, -40 \cdot 2^2,$ $-84, -88 \cdot 2^2, -120, -120 \cdot 2^2, -132, -168, -168 \cdot 2^2, -195, -228, -232 \cdot 2^2,$ $-280, -280 \cdot 2^2, -312, -312 \cdot 2^2, -340, -372, -408, -408 \cdot 2^2, -420, -435,$ $-483, -520, -520 \cdot 2^2, -532, -555, -595, -627, -660, -708, -715,$ $-760, -760 \cdot 2^2, -795, -840, -840 \cdot 2^2, -1012, -1092, -1155, -1320, -1320 \cdot 2^2,$ $-1380, -1428, -1435, -1540, -1848, -1848 \cdot 2^2, -1995, -3003, -3315, -5460$

To state Weinberger's result precisely, denote by D' the square-free part of D :

$$D' = \begin{cases} D, & D \equiv 1 \pmod{4}, \\ D/4, & D \equiv 0 \pmod{4}. \end{cases}$$

Proposition 2.1 (Weinberger [16], Theorem 1) *There exists a negative integer D^* such that for any discriminant D of an imaginary quadratic field the property $|\text{Cl}(D)^2| = 1$ implies $|D'| \leq 5460$ or $D = D^*$.*

Using existing methods [15], it is easy to determine the full list of D with $|\text{Cl}(D)^2| = 1$ and $|D'| \leq 5674$. Since the group $\text{Cl}(D)$ is a quotient of the group $\text{Cl}(Df^2)$, if the latter has property (7) then the former does. Also, for every given D it is easy to find all possible f such that $|\text{Cl}(Df^2)^2| = 1$, using the description of the group $\text{Cl}(Df^2)$ given in Subsection 2.1. Hence the couples (D, f) for which $|\text{Cl}(Df^2)^2| = 1$ and $|D'| \leq 5674$ can be easily listed as well. This list is widely available in the literature since long ago; we reproduce it in Table 2.1.

It follows that Weinberger's result has the following consequence.

Corollary 2.2 *There exists a negative integer D^* such that $|\text{Cl}(Df^2)^2| = 1$ implies that either $\Delta = Df^2$ appears in Table 2.1 or $D = D^*$.*

Remark 2.3 Class numbers of discriminants from Table 2.1 are at most 16, and the results of [15] imply that Table 2.1 contains all Δ with $|\text{Cl}(\Delta)^2| = 1$ and $h(\Delta) \leq 64$. Hence if Δ satisfies $|\text{Cl}(\Delta)^2| = 1$ but does not appear in Table 2.1 then we must have $h(\Delta) \geq 128$.

In particular, the first two lines of Table 2.1 give full lists of negative quadratic discriminants Δ with $h(\Delta) = 1$ and 2.

3 Ring Class Fields and Complex Multiplication

Let K be an imaginary quadratic field, and \mathcal{O} an order in K of discriminant $\Delta = Df^2$. One associates to \mathcal{O} an abelian extension of K with Galois group $\text{Cl}(\mathcal{O})$, called the *ring class field* of \mathcal{O} . We will denote it by $\text{RiCF}(\mathcal{O})$, or $\text{RiCF}(\Delta)$, or $\text{RiCF}(K, f)$. The canonical isomorphism $\text{Cl}(\mathcal{O}) \rightarrow \text{Gal}(\text{RiCF}(\mathcal{O})/K)$ is called the *Artin map*. For the details see, for instance, [7, Section 9].

The correspondence $\mathcal{O} \leftrightarrow \text{RiCF}(\mathcal{O})$ is functorial in the following sense: if \mathcal{O}' is a sub-order of \mathcal{O} then $\text{RiCF}(\mathcal{O}') \subset \text{RiCF}(\mathcal{O})$, and we have the commutative diagram

$$\begin{array}{ccc} \text{Cl}(\mathcal{O}) & \rightarrow & \text{Gal}(\text{RiCF}(\mathcal{O})/K) \\ \downarrow & & \downarrow \\ \text{Cl}(\mathcal{O}') & \rightarrow & \text{Gal}(\text{RiCF}(\mathcal{O}')/K) \end{array}$$

where the horizontal arrows denote Artin maps and the vertical arrows are the natural maps of the class groups and the Galois groups. It follows that the Galois group of $\text{RiCF}(\mathcal{O})$ over $\text{RiCF}(\mathcal{O}')$ is isomorphic to

the kernel of $\text{Cl}(\mathcal{O}) \rightarrow \text{Cl}(\mathcal{O}')$. In particular, $\text{Gal}(\text{RiCF}(\mathcal{O})/\text{RiCF}(\mathcal{O}_K))$ is $\text{Cl}_0(\Delta)$, the group introduced in Subsection 2.1. (One may notice that $\text{RiCF}(\mathcal{O}_K)$ is nothing else but the *Hilbert class field* of K .)

3.1 Compositum of Ring Class Fields

In this subsection it will be more convenient to use the “conductor notation” $\text{RiCF}(K, f)$.

As we have seen above, if $f_1 \mid f$ then $\text{RiCF}(K, f_1) \subset \text{RiCF}(K, f)$. It follows that the compositum of two ring class fields $\text{RiCF}(K, f_1)$ and $\text{RiCF}(K, f_2)$ is a subfield of $\text{RiCF}(K, f)$, where $f = \text{LCM}(f_1, f_2)$. It turns out that this compositum is “almost always” equal to $\text{RiCF}(K, f)$, but there are some exceptions. Here is the precise statement. It is certainly known, but we did not find it in the available literature.

Proposition 3.1 *Let K be an imaginary quadratic field of discriminant D and f_1, f_2 positive integers. Set $f = \text{LCM}(f_1, f_2)$. Then we have the following.*

1. *If $D \neq -3, -4$ then $\text{RiCF}(K, f_1)\text{RiCF}(K, f_2) = \text{RiCF}(K, f)$.*
2. *Assume that $D \in \{-3, -4\}$. Then $\text{RiCF}(K, f_1)\text{RiCF}(K, f_2) = \text{RiCF}(K, f)$ either when one of f_1, f_2 is 1 or when $\gcd(f_1, f_2) > 1$. On the contrary, when $f_1, f_2 > 1$ and $\gcd(f_1, f_2) = 1$, the compositum $\text{RiCF}(K, f_1)\text{RiCF}(K, f_2)$ is a subfield of $\text{RiCF}(K, f)$ of degree 2 for $D = -4$ and of degree 3 for $D = -3$.*

Proof (a sketch). To simplify the notation, we set

$$\begin{aligned} L_0 &= \text{RiCF}(K, 1), & L_1 &= \text{RiCF}(K, f_1), & L_2 &= \text{RiCF}(K, f_2), \\ L &= \text{RiCF}(K, f), & L' &= L_1 L_2. \end{aligned}$$

The mutual position of these fields is illustrated here:

$$\begin{array}{ccccc} & & L_1 & & \\ & \nearrow & \downarrow & \searrow & \\ L_0 & \longrightarrow & L' & \longrightarrow & L \\ & \searrow & \uparrow & \nearrow & \\ & & L_2 & & \end{array}$$

We want to determine the degree $[L : L']$.

We have $\text{Gal}(L/L_0) = \text{Cl}_0(Df^2)$. By (5), this implies

$$\text{Gal}(L/L_0) = (\mathcal{O}_K/f\mathcal{O}_K)^\times / (\mathbb{Z}/f\mathbb{Z})^\times (\mathcal{O}_K^\times)_f,$$

Similarly,

$$\text{Gal}(L_i/L_0) = (\mathcal{O}_K/f_i\mathcal{O}_K)^\times / (\mathbb{Z}/f_i\mathbb{Z})^\times (\mathcal{O}_K^\times)_{f_i} \quad (i = 1, 2).$$

The Galois group $\text{Gal}(L/L_i)$ is the kernel of the natural map

$$(\mathcal{O}_K/f\mathcal{O}_K)^\times / (\mathbb{Z}/f\mathbb{Z})^\times (\mathcal{O}_K^\times)_f \xrightarrow{\pi_i} (\mathcal{O}_K/f_i\mathcal{O}_K)^\times / (\mathbb{Z}/f_i\mathbb{Z})^\times (\mathcal{O}_K^\times)_{f_i}.$$

Hence $\text{Gal}(L/L')$ is the common kernel of the maps π_1 and π_2 . It follows that $\text{Gal}(L/L') = G / (\mathbb{Z}/f\mathbb{Z})^\times (\mathcal{O}_K^\times)_f$, where G is the subgroup of $(\mathcal{O}_K/f\mathcal{O}_K)^\times$ consisting of $x \in (\mathcal{O}_K/f\mathcal{O}_K)^\times$ satisfying

$$x \in (\mathbb{Z}/f\mathbb{Z})(\mathcal{O}_K^\times)_f \pmod{f_i} \quad (i = 1, 2). \quad (8)$$

In particular, $[L : L'] = [G : (\mathbb{Z}/f\mathbb{Z})^\times (\mathcal{O}_K^\times)_f]$.

If $D \neq -3, -4$ then $\mathcal{O}_K^\times = \{\pm 1\}$, which implies that

$$G = (\mathbb{Z}/f\mathbb{Z})^\times (\mathcal{O}_K^\times)_f = (\mathbb{Z}/f\mathbb{Z})^\times$$

and $L = L'$.

Now assume that $D = -4$. Then $\mathcal{O}_K^\times = \{\pm 1, \pm\sqrt{-1}\}$. When $f_1 = 1$ or $f_2 = 1$ the statement is trivial, so we may assume that $f_1, f_2 > 1$. Condition (8) can be re-written as

$$x \in \mathbb{Z}/f\mathbb{Z} \cup (\mathbb{Z}/f\mathbb{Z})\sqrt{-1} \cup ((\mathbb{Z}/f\mathbb{Z})f_1 + (\mathbb{Z}/f\mathbb{Z})f_2\sqrt{-1}) \cup ((\mathbb{Z}/f\mathbb{Z})f_2 + (\mathbb{Z}/f\mathbb{Z})f_1\sqrt{-1}). \quad (9)$$

If $\gcd(f_1, f_2) > 1$ then the last two sets in (9) have no common elements with $(\mathcal{O}_K/f\mathcal{O}_K)^\times$. We obtain

$$G = (\mathbb{Z}/f\mathbb{Z} \cup (\mathbb{Z}/f\mathbb{Z})\sqrt{-1}) \cap (\mathcal{O}_K/f\mathcal{O}_K)^\times = (\mathbb{Z}/f\mathbb{Z})(\mathcal{O}_K^\times)_f,$$

and $L = L'$.

If $\gcd(f_1, f_2) = 1$ then each of the last two sets in (9) has elements belonging to $(\mathcal{O}_K/f\mathcal{O}_K)^\times$ but not to $(\mathbb{Z}/f\mathbb{Z})(\mathcal{O}_K^\times)_f$; for instance $f_1 + f_2\sqrt{-1}$ and $f_2 + f_1\sqrt{-1}$, respectively (here we use the assumption $f_1, f_2 > 1$). Hence $[G : (\mathbb{Z}/f\mathbb{Z})(\mathcal{O}_K^\times)_f] > 1$. On the other hand, if x and y belong to the last two sets in (9), then $xy \in \mathbb{Z}/f\mathbb{Z}$ if they belong to the same set, and $xy \in (\mathbb{Z}/f\mathbb{Z})\sqrt{-1}$ if they belong to distinct sets. This shows that $[G : (\mathbb{Z}/f\mathbb{Z})(\mathcal{O}_K^\times)_f] = 2$, and hence $[L : L'] = 2$. This completes the proof in the case $D = -4$.

The case $D = -3$ is treated similarly. We omit the details. \square

3.2 Complex Multiplication

Ring class fields are closely related to the Complex Multiplication. Let $\tau \in K$ with $\text{Im}\tau > 0$ be such that $\mathcal{O} = \text{End}\langle\tau, 1\rangle$ (where $\langle\tau, 1\rangle$ is the lattice generated by τ and 1); one says that \mathcal{O} is the *complex multiplication order* of the lattice $\langle\tau, 1\rangle$.

The ‘‘Main Theorem of Complex Multiplication’’ asserts that $j(\tau)$ is an algebraic integer generating over K the ring class field $\text{RiCF}(\mathcal{O})$. In particular, $[K(j(\tau)) : K] = h(\mathcal{O})$. In fact, one has more:

$$[K(j(\tau)) : K] = [\mathbb{Q}(j(\tau)) : \mathbb{Q}] = h(\mathcal{O}). \quad (10)$$

The proofs can be found in many sources; see, for instance, [7, Section 11].

Since $\text{RiCF}(\Delta) = K(j(\tau))$ is a Galois extension of K , it contains, by (10), all the \mathbb{Q} -conjugates of $j(\tau)$. It follows that $K(j(\tau))$ is Galois over \mathbb{Q} ; in particular, the Galois group $\text{Gal}(K/\mathbb{Q})$ acts on $\text{Gal}(K(j(\tau))/K)$.

Proposition 3.2 *The Galois group $\text{Gal}(K/\mathbb{Q})$ acts on $\text{Gal}(K(j(\tau))/K)$ ‘‘dihedrally’’: if ι is the non-trivial element of $\text{Gal}(K/\mathbb{Q})$, then we have $\sigma^\iota = \sigma^{-1}$ for any $\sigma \in \text{Gal}(K(j(\tau))/K)$.*

For a proof see, for instance [7, Lemma 9.3].

Corollary 3.3 *The following properties are equivalent.*

1. *The field $K(j(\tau))$ is abelian over \mathbb{Q} .*
2. *The Galois group $\text{Gal}(K(j(\tau))/K)$ is annihilated by 2 (that is, isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \cdots \times \mathbb{Z}/2\mathbb{Z}$).*
3. *The Galois group $\text{Gal}(K(j(\tau))/\mathbb{Q})$ is annihilated by 2.*
4. *The field $\mathbb{Q}(j(\tau))$ is Galois over \mathbb{Q} .*
5. *The field $\mathbb{Q}(j(\tau))$ is abelian over \mathbb{Q} .*

Proof. The implications $1 \Rightarrow 2 \Rightarrow 3$ follow from Proposition 3.2. The implication $3 \Rightarrow 4$ is trivial. To see the implication $4 \Rightarrow 5$, just observe that (10) implies the isomorphism $\text{Gal}(K(j(\tau))/K) \cong \text{Gal}(\mathbb{Q}(j(\tau))/\mathbb{Q})$. Finally, the implication $5 \Rightarrow 1$ is again trivial. \square

3.3 The Conjugates of $j(\tau)$

Let τ and \mathcal{O} be as in Subsection 3.2, and let Δ be the discriminant of \mathcal{O} . As we already mentioned in the beginning of Subsection 3.2, $j(\tau)$ is an algebraic integer of degree $h(\Delta)$. It is well-known that the \mathbb{Q} -conjugates of $j(\tau)$ can be described explicitly. Below we briefly recall this description.

Denote by $T = T_\Delta$ the set of triples of integers (a, b, c) such that

$$\begin{aligned} \gcd(a, b, c) &= 1, \quad \Delta = b^2 - 4ac, \\ \text{either } -a < b \leq a < c \quad \text{or} \quad 0 \leq b \leq a = c \end{aligned}$$

Proposition 3.4 *All \mathbb{Q} -conjugates of $j(\tau)$ are given by*

$$j\left(\frac{-b + \sqrt{\Delta}}{2a}\right), \quad (a, b, c) \in T_\Delta. \quad (11)$$

In particular, $h(\Delta) = |T_\Delta|$.

For a proof, see, for instance, [7, Theorem 7.7].

The following observation will be crucial: in the set T_Δ there exists exactly one triple (a, b, c) with $a = 1$. This triple can be given explicitly: it is

$$\left(1, r_4(\Delta), \frac{r_4(\Delta) - \Delta}{4}\right),$$

where $r_4(\Delta) \in \{0, 1\}$ is defined by $\Delta \equiv r_4(\Delta) \pmod{4}$. The corresponding number $j(\tau)$, where

$$\tau = \frac{-r_4(\Delta) + \sqrt{\Delta}}{2},$$

will be called *the dominant j -value* of discriminant Δ . It is important for us that it is much larger in absolute value than all its conjugates.

Lemma 3.5 *Let $j(\tau)$ be the dominant j -value of discriminant Δ , with $|\Delta| \geq 11$, and let $j(\tau') \neq j(\tau)$ be conjugate to $j(\tau)$ over \mathbb{Q} . Then $|j(\tau')| \leq 0.1|j(\tau)|$.*

Proof. Recall the inequality $||j(z)| - |q_z^{-1}|| \leq 2079$, where $q_z = e^{2\pi iz}$, for z belonging to the standard fundamental domain of $\text{SL}_2(\mathbb{Z})$ on the Poincaré plane [4, Lemma 1]. We may assume that $\tau = (-r_4(\Delta) + \sqrt{\Delta})/2$ and $\tau' = (-b + \sqrt{\Delta})/2a$ with $a \geq 2$. Hence $|q_\tau| = e^{\pi\sqrt{|\Delta|}} \geq e^{\pi\sqrt{11}} > 33506$ and $|q_{\tau'}| \leq |q_\tau|^{1/2}$. We obtain

$$\frac{|j(\tau')|}{|j(\tau)|} \leq \frac{|q_\tau|^{1/2} + 2079}{|q_\tau| - 2079} \leq \frac{33506^{1/2} + 2079}{33506 - 2079} < 0.1,$$

as wanted. \square

The minimal polynomial of $j(\tau)$ over \mathbb{Z} is called the *Hilbert class polynomial*² of discriminant Δ ; it indeed depends only on Δ because its roots are the numbers (11). We will denote it $H_\Delta(x)$.

4 Comparing two CM-fields

In this section we study the field equality $\mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2))$. We distinguish two cases: $\mathbb{Q}(\tau_1) \neq \mathbb{Q}(\tau_2)$, where we obtain the complete list of all possibilities, and $\mathbb{Q}(\tau_1) = \mathbb{Q}(\tau_2)$, where we will see that Δ_1 and Δ_2 are “almost the same”. Here for $i = 1, 2$ we denote by Δ_i the discriminant of the “complex multiplication order” $\mathcal{O}_i = \text{End}(\tau_i, 1)$, and write $\Delta_i = D_i f_i^2$ with the obvious meaning of D_i and f_i .

²or, sometimes, *ring class polynomial*, to indicate that its root generates not the Hilbert class field, but the more general ring class field

4.1 The case $\mathbb{Q}(\tau_1) \neq \mathbb{Q}(\tau_2)$

In this subsection we investigate the case when $\mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2))$, but the fields $\mathbb{Q}(\tau_1)$ and $\mathbb{Q}(\tau_2)$ are distinct. It turns out that this is a very strong condition, which leads to a completely explicit characterization of all possible cases.

Theorem 4.1 *Let τ_1 and τ_2 be quadratic numbers such that $\mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2))$, but $\mathbb{Q}(\tau_1) \neq \mathbb{Q}(\tau_2)$. Then both Δ_1 and Δ_2 appear in Table 2.1.*

Proof. Denote by L the field $\mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2))$. If L is a Galois extension of \mathbb{Q} , then the group $\text{Cl}(\Delta_1) = \text{Cl}(\Delta_2)$ is annihilated by 2 by Corollary 3.3, and we can use Corollary 2.2. Since $D_1 \neq D_2$, at least one of the two discriminants D_1 and D_2 is distinct from D^* ; say, $D_1 \neq D^*$. Then Δ_1 is in Table 2.1. Since $h(\Delta_1) = h(\Delta_2)$, Remark 2.3 implies that Δ_2 is in Table 2.1 as well. (This argument goes back to Kühne [10, Section 6].)

Now assume that

$$L \text{ is not Galois over } \mathbb{Q}. \quad (12)$$

We will show that this leads to a contradiction. Denote by M the Galois closure of L over \mathbb{Q} ; then $M = \mathbb{Q}(\tau_1, j(\tau_1)) = \mathbb{Q}(\tau_2, j(\tau_2))$. Define the Galois groups

$$\begin{aligned} G &= \text{Gal}(M/\mathbb{Q}), & \tilde{N} &= \text{Gal}(M/\mathbb{Q}(\tau_1, \tau_2)), \\ N_i &= \text{Gal}(M/\mathbb{Q}(\tau_i)) = \text{Cl}(\Delta_i) \quad (i = 1, 2), \end{aligned}$$

so that $\tilde{N} = N_1 \cap N_2$ and $[N_1 : \tilde{N}] = [N_2 : \tilde{N}] = 2$.

We claim the following:

$$\text{the group } \tilde{N} \text{ is annihilated by 2.} \quad (13)$$

(One may mention that this is a special case of an observation made independently by Edixhoven [8] and André [1].)

Indeed, let ι_1 be an element of G acting non-trivially on τ_1 but trivially on τ_2 . Then for any $\sigma \in N_1$ we have $\sigma^{\iota_1} = \sigma^{-1}$ by Proposition 3.2. On the other hand, for any $\sigma \in N_2$ we have $\sigma^{\iota_1} = \sigma$. It follows that $\sigma = \sigma^{-1}$ for $\sigma \in \tilde{N}$, proving (13).

Thus, each of the groups N_1 and N_2 has a subgroup of index 2 isomorphic to $(\mathbb{Z}/2\mathbb{Z})^\mu$ for some integer μ . Hence each of N_1 and N_2 is isomorphic either to $(\mathbb{Z}/2\mathbb{Z})^{\mu+1}$ or to $\mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^{\mu-1}$.

If, say, $N_1 \cong (\mathbb{Z}/2\mathbb{Z})^{\mu+1}$ then L is Galois over \mathbb{Q} by Corollary 3.3, contradicting (12). Therefore

$$N_1 \cong N_2 \cong \mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^{\mu-1}.$$

Let $\iota \in G$ be the complex conjugation. Since i extends the non-trivial element of $\text{Gal}(\mathbb{Q}(\tau_1)/\mathbb{Q})$, the group $H = \{1, \iota\}$ acts on N_1 dihedrally: $\sigma^\iota = \sigma^{-1}$ for $\sigma \in N_1$, and we have $G = N_1 \rtimes H$. Let N'_1 and N''_1 be subgroups of N_1 isomorphic to $\mathbb{Z}/4\mathbb{Z}$ and $(\mathbb{Z}/2\mathbb{Z})^{\mu-1}$, respectively, such that $N_1 = N'_1 \times N''_1$. Then H commutes with N''_1 and acts dihedrally on N'_1 . Hence

$$G = N_1 \rtimes H = (N'_1 \rtimes H) \times N''_1 \cong D_8 \times (\mathbb{Z}/2\mathbb{Z})^{\mu-1},$$

where D_{2n} denotes the dihedral group of $2n$ elements.

Now observe that $D_8 \times (\mathbb{Z}/2\mathbb{Z})^{\mu-1}$ has only one subgroup isomorphic to the group $\mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^{\mu-1}$; this follows, for instance, from the fact that both groups have exactly 2^μ elements of order 4. Hence $N_1 = N_2$, which implies the equality $\mathbb{Q}(\tau_1) = \mathbb{Q}(\tau_2)$, a contradiction. \square

Now one can go further and, inspecting all possible pairs of fields, produce the full list of number fields presented as $\mathbb{Q}(j(\tau_1))$ and $\mathbb{Q}(j(\tau_2))$ with $\mathbb{Q}(\tau_1) \neq \mathbb{Q}(\tau_2)$.

Corollary 4.2 *Let L be a number field with the following property: there exist quadratic τ_1 and τ_2 such that $L = \mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2))$ but $\mathbb{Q}(\tau_1) \neq \mathbb{Q}(\tau_2)$. Then L is one of the fields in Table 4.1.*

Table 4.1: Fields presented as $\mathbb{Q}(j(\tau_1))$ and $\mathbb{Q}(j(\tau_2))$ with $\mathbb{Q}(\tau_1) \neq \mathbb{Q}(\tau_2)$

Field L	$[L : \mathbb{Q}]$	Δ	$\text{Cl}(\Delta)$
\mathbb{Q}	1	$-3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163$	trivial
$\mathbb{Q}(\sqrt{2})$	2	$-24, -32, -64, -88$	$\mathbb{Z}/2\mathbb{Z}$
$\mathbb{Q}(\sqrt{3})$	2	$-36, -48$	$\mathbb{Z}/2\mathbb{Z}$
$\mathbb{Q}(\sqrt{5})$	2	$-15, -20, -35, -40, -60, -75, -100, -115, -235$	$\mathbb{Z}/2\mathbb{Z}$
$\mathbb{Q}(\sqrt{13})$	2	$-52, -91, -403$	$\mathbb{Z}/2\mathbb{Z}$
$\mathbb{Q}(\sqrt{17})$	2	$-51, -187$	$\mathbb{Z}/2\mathbb{Z}$
$\mathbb{Q}(\sqrt{2}, \sqrt{3})$	4	$-96, -192, -288$	$(\mathbb{Z}/2\mathbb{Z})^2$
$\mathbb{Q}(\sqrt{3}, \sqrt{5})$	4	$-180, -240$	$(\mathbb{Z}/2\mathbb{Z})^2$
$\mathbb{Q}(\sqrt{5}, \sqrt{13})$	4	$-195, -520, -715$	$(\mathbb{Z}/2\mathbb{Z})^2$
$\mathbb{Q}(\sqrt{2}, \sqrt{5})$	4	$-120, -160, -280, -760$	$(\mathbb{Z}/2\mathbb{Z})^2$
$\mathbb{Q}(\sqrt{5}, \sqrt{17})$	4	$-340, -595$	$(\mathbb{Z}/2\mathbb{Z})^2$
$\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$	8	$-480, -960$	$(\mathbb{Z}/2\mathbb{Z})^3$

Explanations:

1. the third column contains the full list of discriminants Δ of CM-orders $\text{End}(\tau, 1)$ such that $L = \mathbb{Q}(j(\tau))$;
2. the fourth column gives the structure of the class group $\text{Cl}(\Delta)$ for any such Δ .

Proof. This is just a calculation using PARI. □

4.2 The case $\mathbb{Q}(\tau_1) = \mathbb{Q}(\tau_2)$

Now assume that $\mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2))$ and $\mathbb{Q}(\tau_1) = \mathbb{Q}(\tau_2)$. Denote by D be the discriminant of the number field $\mathbb{Q}(\tau_1) = \mathbb{Q}(\tau_2)$ and write $\Delta_i = f_i^2 D$ for $i = 1, 2$.

Proposition 4.3 *Assume that $\mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2))$ and $\mathbb{Q}(\tau_1) = \mathbb{Q}(\tau_2)$. Then either*

$$f_1/f_2 \in \{1, 2, 1/2\} \quad (14)$$

or $D = -3$ and $f_1, f_2 \in \{1, 2, 3\}$ (in which cases $\mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2)) = \mathbb{Q}$).

Proof. Put $f = \text{LCM}(f_1, f_2)$. When $D \neq -3, -4$, Proposition 3.1 implies that

$$h(f^2 D) = [\mathbb{Q}(\sqrt{D}, j(\tau_1), j(\tau_2)) : \mathbb{Q}(\sqrt{D})] \quad (15)$$

Since $j(\tau_1)$ and $j(\tau_2)$ generate the same field, we obtain

$$h(f_1^2 D) = h(f_2^2 D) = h(f^2 D). \quad (16)$$

Using (6) and (16), we obtain

$$\frac{f}{f_1} \prod_{\substack{p|f \\ p \nmid f_1}} \left(1 - \left(\frac{D}{p}\right) p^{-1}\right) = 1,$$

which implies that $f/f_1 \in \{1, 2\}$. Similarly, $f/f_2 \in \{1, 2\}$. Hence we have (14).

Now assume that $D \in \{-3, -4\}$. If $\gcd(f_1, f_2) > 1$ then we again have (15), and the same argument proves (14).

If, say, $f_1 = 1$ then either $D = -4$ and $f_2 \in \{1, 2\}$, in which case we again have (14), or $D = -3$ and $f_2 \in \{1, 2, 3\}$.

Finally, assume that $f_1, f_2 > 1$ and $\gcd(f_1, f_2) = 1$. Then $f = f_1 f_2$ and Proposition 3.1 implies that

$$h(f_1^2 D) = h(f_2^2 D) = \ell^{-1} h(f^2 D), \quad (17)$$

where $\ell = 2$ for $D = -4$ and $\ell = 3$ for $D = -3$. Using (6) and (17), we obtain

$$f_i \prod_{p|f_i} \left(1 - \left(\frac{D}{p}\right) p^{-1}\right) = \ell \quad (i = 1, 2),$$

and a quick inspection shows that in this case $D = -3$ and $\{f_1, f_2\} = \{2, 3\}$. \square

5 Proof of Theorem 1.2

We assume that $P = (j(\tau_1), j(\tau_2))$ belongs to a non-special straight line ℓ defined over \mathbb{Q} , and show that it satisfies either (2) or (3). We define $\Delta_i = D_i f_i^2$ as in the beginning of Section 4.

Let $A_1 x_1 + A_2 x_2 + B = 0$ be the equation of ℓ . Since ℓ is not special, we have $A_1 A_2 \neq 0$, which implies, in particular, that

$$\mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2)). \quad (18)$$

We set

$$L = \mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2)), \quad h = h(\Delta_1) = h(\Delta_2) = [L : \mathbb{Q}].$$

If $j(\tau_1), j(\tau_2) \in \mathbb{Q}$ (that is, $h = 1$) we are done. From now on assume that

$$j(\tau_1), j(\tau_2) \notin \mathbb{Q}.$$

If $j(\tau_1) = j(\tau_2)$ then ℓ is the special line $x_1 = x_2$, because it passes through the points $(j(\tau_1), j(\tau_1))$ and through all its conjugates over \mathbb{Q} . Hence

$$j(\tau_1) \neq j(\tau_2). \quad (19)$$

If $h = 2$ then we have (3). From now on assume that

$$h \geq 3, \quad (20)$$

and, in particular,

$$|\Delta_1|, |\Delta_2| \geq 23. \quad (21)$$

We will show that this leads to a contradiction.

Remark 5.1 Before proceeding with the proof, remark that, for a given pair of distinct discriminants Δ_1 and Δ_2 it is easy to verify whether there exists a point $(j(\tau_1), j(\tau_2))$ on a non-special straight line defined over \mathbb{Q} , such that Δ_i is the discriminant of the CM-order $\text{End}(\tau_i, 1)$. Call two polynomials $f(x), g(x) \in \mathbb{Q}[x]$ *similar* if there exist $\alpha, \beta, \lambda \in \mathbb{Q}$ with $\alpha\lambda \neq 0$ such that $f(\alpha x + \beta) = \lambda g(x)$. Now, a point $(j(\tau_1), j(\tau_2))$ as above exists if and only if the class polynomials H_{Δ_1} and H_{Δ_2} (see end of Subsection 3.3) are similar. This can be easily verified using, for instance, the PARI package.

5.1 Both Coordinates are Dominant

It turns out that we may assume, without a loss of generality, that both $j(\tau_1)$ and $j(\tau_2)$ are the *dominant* j -values of corresponding discriminants, as defined in Subsection 3.3.

Lemma 5.2 *Assume that ℓ is a non-special straight line containing a CM-point $P = (j(\tau_1), j(\tau_2))$ satisfying (18), (19) and (20). Then ℓ contains a CM-point $P' = (j(\tau'_1), j(\tau'_2))$, conjugate to P over \mathbb{Q} and such that $j(\tau'_i)$ is the dominant j -value of discriminant Δ_i for $i = 1, 2$.*

Proof. Since ℓ is defined over \mathbb{Q} , all \mathbb{Q} -conjugates of P belong to ℓ as well. Replacing P by a \mathbb{Q} -conjugate point, we may assume that $j(\tau_1)$ is the dominant j -value for the discriminant Δ_1 . If $j(\tau_2)$ is the dominant value for Δ_2 we are done; so assume it is not, and show that this leads to a contradiction.

Since both $j(\tau_1)$ and $j(\tau_2)$ generate the same field of degree h over \mathbb{Q} , the Galois orbit of P (over \mathbb{Q}) has exactly h elements; moreover, each conjugate of $j(\tau_1)$ occurs exactly once as the first coordinate of a point in the orbit, and each conjugate of $j(\tau_2)$ occurs exactly once as the second coordinate.

It follows that there is a conjugate point P^σ such that the second coordinate $j(\tau_2)^\sigma$ is the dominant j -value for Δ_2 ; then its first coordinate $j(\tau_1)^\sigma$ is not dominant for Δ_1 because $P^\sigma \neq P$. Since $h \geq 3$, there exists yet another point $P^{\sigma'}$ with both coordinates not dominant for the respective discriminants.

All three points P , P^σ and $P^{\sigma'}$ belong to ℓ . Hence

$$\begin{vmatrix} 1 & j(\tau_1) & j(\tau_2) \\ 1 & j(\tau_1)^\sigma & j(\tau_2)^\sigma \\ 1 & j(\tau_1)^{\sigma'} & j(\tau_2)^{\sigma'} \end{vmatrix} = 0.$$

The determinant above is a sum of 6 terms: the “dominant term” $j(\tau_1)j(\tau_2)^\sigma$ and 5 other terms. Each of the other terms is at most $0.1|j(\tau_1)j(\tau_2)^\sigma|$ in absolute value: this follows from Lemma 3.5, which applies here due to (21). Hence the determinant cannot vanish, a contradiction. \square

5.2 Completing the proof

After this preparation, we are ready to complete the proof of Theorem 1.2. Thus, let $P = (j(\tau_1), j(\tau_2))$ belong to a straight line ℓ defined over \mathbb{Q} . We assume that (18), (19) and (20) are satisfied, and we may further assume that $j(\tau_1)$, $j(\tau_2)$ are the dominant j -values of Δ_1 , Δ_2 , respectively.

If $\mathbb{Q}(\tau_1) \neq \mathbb{Q}(\tau_2)$ then Corollary 4.2 applies, and all possible L , Δ_1 and Δ_2 can be found in Table 4.1. In particular, we have only 6 possible fields L and 15 possible couples Δ_1, Δ_2 . All of the latter are ruled out by verifying (using PARI) that the corresponding Hilbert class polynomials $H_{\Delta_1}(x)$ and $H_{\Delta_2}(x)$ are not similar, as explained in Remark 5.1.

If $\mathbb{Q}(\tau_1) = \mathbb{Q}(\tau_2)$ then Proposition 4.3 applies, and we have $f_1/f_2 \in \{1, 2, 1/2\}$. Since both $j(\tau_1)$ and $j(\tau_2)$ are dominant, the case $f_1 = f_2$ is impossible: there is only one dominant j -value for every given discriminant, and we have $j(\tau_1) \neq j(\tau_2)$ by (19). Thus, $f_1/f_2 \in \{2, 1/2\}$.

Assume, for instance, that $f_2 = 2f_1$. Write $\Delta_2 = \Delta$, so that $\Delta_1 = 4\Delta$. Since both $j(\tau_1)$ and $j(\tau_2)$ are dominant, we may choose

$$\tau_1 = \frac{-r_4(4\Delta) + \sqrt{4\Delta}}{2} = \sqrt{\Delta}, \quad \tau_2 = \frac{-r_4(\Delta) + \sqrt{\Delta}}{2}$$

It follows that $\tau_2 = \frac{1}{2}\gamma(\tau_1)$, where

$$\gamma = \begin{pmatrix} 1 & -r_4(\Delta) \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Hence the point $P = (j(\tau_1), j(\tau_2))$ belongs to the modular curve $Y_0(2)$ realized as the plane curve $\Phi_2(x_1, x_2) = 0$, where

$$\begin{aligned} \Phi_2(x_1, x_2) = & -x_1^2x_2^2 + x_1^3 + x_2^3 + 1488x_1^2x_2 + 1488x_1x_2^2 + 40773375x_1x_2 \\ & - 162000x_1^2 - 162000x_2^2 + 8748000000x_1 + 8748000000x_2 \\ & - 15746400000000 \end{aligned}$$

is the modular polynomial of level 2. Since $\deg \Phi_2 = 4$ and P belongs to a straight line over \mathbb{Q} , the coordinates of P generate a field of degree at most 4 over \mathbb{Q} . Thus, $3 \leq h \leq 4$.

Looking into existing class number tables (or using PARI) one finds that there exist only 5 negative discriminants Δ such that $h(\Delta) = h(4\Delta) \in \{3, 4\}$:

$$\begin{aligned} h = 3 : & \quad -23, -31; \\ h = 4 : & \quad -7 \cdot 3^2, -39, -55. \end{aligned}$$

Verifying that the polynomials H_Δ and $H_{4\Delta}$ for these values of Δ are not similar is an easy calculation with PARI. \square

Remark 5.3 We conclude the article with some computational remarks.

1. As indicated in the introduction, it is very easy to list all CM-points satisfying (2) or (3); call them *rational* and *quadratic*, respectively.

There exist exactly 13 discriminants Δ with $h(\Delta) = 1$, the first line of Table 2.1 lists them all. Hence there exist 169 rational CM-points, and listing them explicitly is plainly straightforward.

As for the quadratic CM-points, there are two kinds of them: points with

$$\Delta_1 = \Delta_2 = \Delta, \quad h(\Delta) = 2, \quad j(\tau_1) \text{ and } j(\tau_2) \text{ are conjugate over } \mathbb{Q}, \quad (22)$$

and points with

$$\Delta_1 \neq \Delta_2, \quad h(\Delta_1) = h(\Delta_2) = 2, \quad \mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2)). \quad (23)$$

There exist exactly 29 negative quadratic discriminants Δ with $h(\Delta) = 2$, see the second line of Table 2.1 for the complete list. Hence there exist 29, up to conjugacy, quadratic CM-points satisfying (22).

The quadratic CM-points satisfying (23) can be extracted from the “quadratic” part of Table 4.1. Indeed, if $\mathbb{Q}(\tau_1) \neq \mathbb{Q}(\tau_2)$ then Δ_1, Δ_2 are in Table 4.1 by Corollary 4.2. And if $\mathbb{Q}(\tau_1) = \mathbb{Q}(\tau_2)$ then $\Delta_1/\Delta_2 \in \{4, 1/4\}$ by Proposition 4.3. Inspecting the list of the 29 discriminants with $h(\Delta) = 2$, we find that the only possibility is $\{\Delta_1, \Delta_2\} = \{-15, -60\}$. Both these values appear in Table 4.1 in the line corresponding to the field $\mathbb{Q}(\sqrt{5})$.

Looking into Table 4.1 we find that there exist

$$4(4-1) + 2(2-1) + 9(9-1) + 3(3-1) + 2(2-1) = 94$$

(ordered) pairs (Δ_1, Δ_2) as in (23). Each pair gives rise to two, up to conjugacy, points satisfying (23). So, up to conjugacy, there are 188 points satisfying (23), and $188 + 29 = 217$ quadratic CM-points altogether. Again, listing them explicitly is a straightforward computation.

2. Thomas Scanlon (private communication) asked whether there exists a non-special straight line over \mathbb{C} passing through more than 2 CM-points. Since

$$\det \begin{bmatrix} 1728 & -884736000 \\ 287496 & -147197952000 \end{bmatrix} = 0,$$

the points $(0,0)$, $(1728, 287496)$ and $(-884736000, -147197952000)$ belong to the same straight line, and so do the points $(0,0)$, $(1728, -884736000)$ and $(287496, -147197952000)$. Notice that

$$\begin{aligned} j\left(\frac{-1 + \sqrt{-3}}{2}\right) &= 0, \quad j(\sqrt{-1}) = 1728, \quad j(2\sqrt{-1}) = 287496, \\ j\left(\frac{-1 + \sqrt{-43}}{2}\right) &= -884736000, \quad j\left(\frac{-1 + \sqrt{-67}}{2}\right) = -147197952000. \end{aligned}$$

We verified that (up to switching the variables x_1, x_2) these are the only such lines defined over \mathbb{Q} . Precisely:

- no 3 rational CM-points, with the exceptions indicated above, lie on the same non-special line;
- no line passing through conjugate quadratic CM-points contains a rational CM-point;
- lines defined by pairs of conjugate quadratic CM-points are all pairwise distinct.

The verification is a quick calculation with PARI.

It is not clear to us whether the examples above (and absence of other examples) are just accidental, or admit some conceptual explanations.

3. All the computations for this paper take about 20 seconds.

References

- [1] Y. ANDRÉ, Finitude des couples d’invariants modulaires singuliers sur une courbe algébrique plane non modulaire, *J. Reine Angew. Math.* **505** (1998), 203–208.
- [2] A. BAJOLET, Finding singular moduli on a complex line, *Int. J. Number Theory* **10** (2014), 763–777.
- [3] YU. BILU, F. LUCA, A. PIZARRO-MADARIAGA, Rational Products of Singular Moduli, submitted; [arXiv:1410.1806](#) .
- [4] YU. BILU, D. MASSER, U. ZANNIER, An effective “Theorem of André” for CM-points on a plane curve, *Math. Proc. Cambridge Philos. Soc.* **154** (2013), 145–152.
- [5] F. BREUER, Heights of CM points on complex affine curves, *Ramanujan J.* **5** (2001), 311–317.
- [6] S. CHOWLA, An extension of Heilbronn’s class-number theorem, *Quat. J. Math. Oxford* **5**, 304–307.
- [7] D. A. COX, *Primes of the form $x^2 + ny^2$* , Wiley, NY, 1989.
- [8] B. EDIXHOVEN, Special points on the product of two modular curves, *Compos. Math.* **114** (1998), 315–328.
- [9] L. KÜHNE An effective result of André-Oort type *Ann. Math. (2)* **176** (2012), 651–671.
- [10] L. KÜHNE An effective result of André-Oort type II, *Acta Arith.* **161** (2013), 1–19.
- [11] J. PILA, Rational points of definable sets and results of André-Oort-Manin-Mumford type, *Int. Math. Res. Notices* 2009, 2476–2507.
- [12] J. PILA, O-minimality and the André-Oort conjecture for \mathbb{C}^n , *Ann. Math. (2)* **173** (2011), 1779–1840.
- [13] J. PILA, U. ZANNIER, Rational points in periodic analytic sets and the Manin-Mumford conjecture. *Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei (9) Mat. Appl.* **19** (2008), 149–162.
- [14] T. TATUZAWA, On a Theorem of Siegel, *Jap. J. Math.* **21** (1951), 163–178 (1952).
- [15] M. WATKINS, Class numbers of imaginary quadratic fields, *Math. Comp.* **73** (2004), 907–938.
- [16] P. J. WEINBERGER, Exponents of the class group of the complex quadratic fields, *Acta Arith.* **22** (1973), 117–123.
- [17] THE PARI GROUP, PARI/GP version 2.7.1 (2014), Bordeaux; available from <http://pari.math.u-bordeaux.fr/>.

Bill Allombert

Université de Bordeaux
IMB, UMR 5251
F-33400 Talence, France

CNRS

IMB, UMR 5251
F-33400 Talence, France

INRIA

F-33400 Talence, France

Yuri Bilu

Institut de Mathématiques de Bordeaux
Université de Bordeaux
351 cours de la Libération
33405 Talence, France

Amalia Pizarro-Madariaga

Instituto de Matemáticas
Universidad de Valparaíso
Chile